DDI谛听

深度学习在无人机方向监测中的应用

Deep Learning in Drone Direction Indication

汇报：刘诗楠

时间：2017年8月25日

CONTENTS

目　　录

1

PART 01

无人机攻防背景

从无线电角度而言

无线电反无人机技术

控制信号干扰与欺骗

屏蔽或中间人攻击2.4GHz或5.8GHz的WiFi信号，信号的丢失迫使飞机进入丢失的链路状态，开启自动返航模式。

GPS屏蔽与欺骗

360 Unicorn团队已经证明了针对无人机的低成本GPS欺骗能带来相应的效果

操纵相机捕获的图像

低空无人机依靠摄像机拍摄的视频进行导航和避障

ADS-B信号欺骗

平民无人机已配备自动相关监视广播（ADS-B）系统，每秒播放飞机的位置和速度，以避免与其他载人或无人飞机相撞

注入伪造的传感器数据

在飞行控制器中注入制造的读数来破坏一组传感器，操纵所有外部影响的传感器，如雷达，红外和电光传感器

拒绝服务攻击

通过数据链路以随机命令淹没其网卡可能迫使这种无人机进入意外的状态

无线电反无人机应用

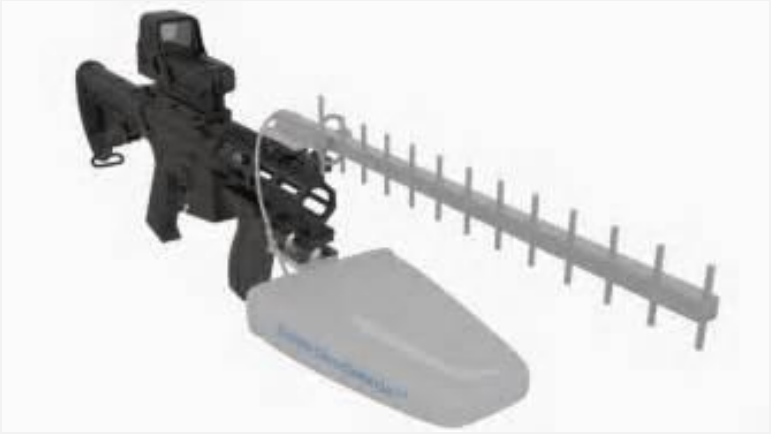
无人机防御者

Drone Defender

首款可精准快速阻止可疑无人机靠近的、可移动的非破坏性反无人机专用设备。该设备有效打击范围为400米，仅对依靠GPS导航或实时遥控的无人机有效（如四轴和六轴飞行器）。

SkyJack

Kamkar于2013年在Github上发布了名为SkyJack的Perl软件，运行在 Raspberry Pi上并使用其它开源软件来劫持飞行器。



“蒂奴皮”E1000MP便携式干扰器总输出功率超过100瓦，共有五个频道，采用GPS中断和定向电子对抗干扰技术，诱使无人机离开保护区或自动着陆。

雷达

那么，如何检测无人机的存在呢？

Drone Detection

- 计算机视觉
- 无线电监控
- 雷达
- 声音感知

……

无人机检测：雷达 Drone Detection：Radar

黑睿技术公司UAVX系统的人工智能系统连接雷达以及其他的传感器，使用神经网络人工智能进行自动分类检测，在实时绘图软件用真实数据对人工智能进行训练。

UAVX系统的工作流程主要包括探测、情报、分类、警告，首先使用小型监视雷达探测500米范围内的中型无人机，一旦有目标进入探测范围，系统可产生数百个雷达反射数据样本；同时UAVX系统将目标特性与数据库中数千种预先训练好的常见无人机类型进行对比，每一次交互的证据数据都会保存下来，可实时通过浏览器查看亦可事后查看。

无人机检测：计算机视觉 Drone Detection：Computer Vision

计算机视觉技术一般在视距范围内对雷达进行辅助，包括紫外成像、可见光成像、近红外光谱(NIR)成像等技术。该类技术的优点包括成本低、可用商用现货充足、视场灵活性较高；缺点包括受杂波影响严重、夜间效果差（需要主动照射），受天气影响严重。

无人机检测：声音感知 Drone Detection：Sound Cognition

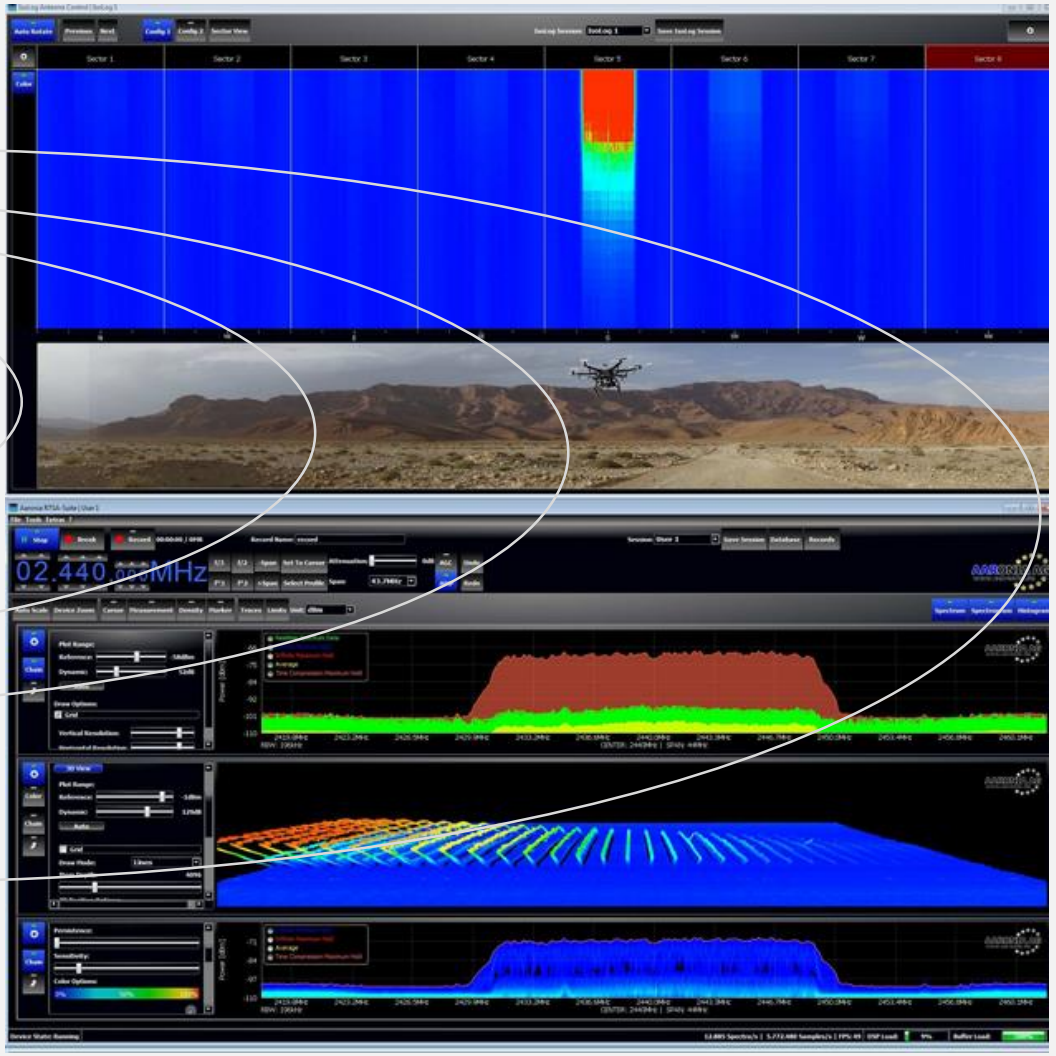
Drone Shield采用的是声音感知技术。目前该企业的技术可以实现的声音识别距离达到了1公里。

它内置了Raspberry Pi、信号处理器、麦克风、分析软件、无人机声音特性的数据库，通过监听周围环境的声音，通过声音对比确定是否有无人机。当有无人机在附近时，通过邮件或者短信发出警报。从原理上来看，并不难。

无人机检测：无线监测 Drone Detection：Wireless Monitoring

安诺尼多点解决方案由多个天线和实时频谱仪组成，然后集中在一台监控计算机上同时管理所有系统。多点解决方案的优点是可实现三角测量定位，这样可以实现非常高的跟踪精度。

无人机侦测软件提供直观界面设计，结合强大的跟踪、触发、显示功能选件来帮助识别，捕获和跟踪从无人机或其它射频信号源高达20GHZ的射频辐射。每个扇区/天线都有自己的实时视图，用于识别无人机的准确方向。



2

PART 02

作品设计及实现

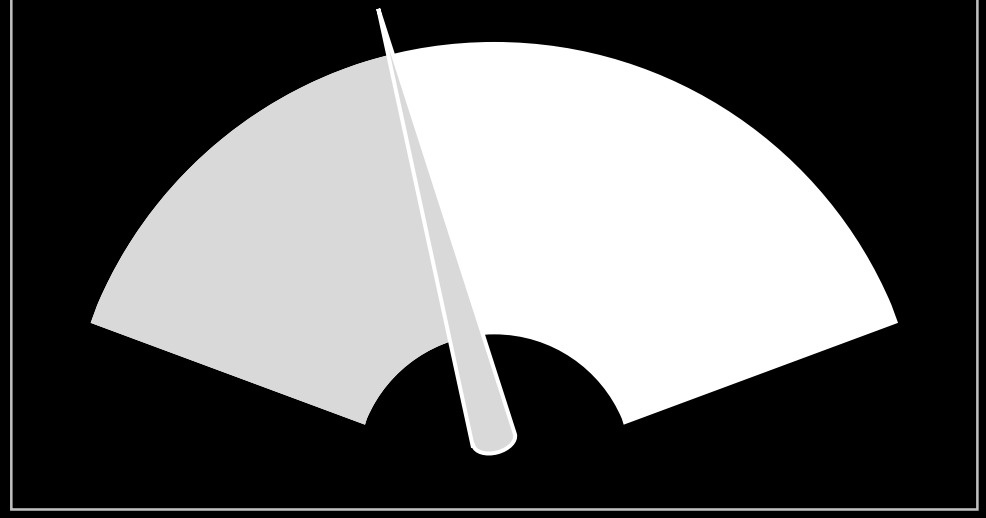
发现

方向识别技术

声音感知、雷达

问题

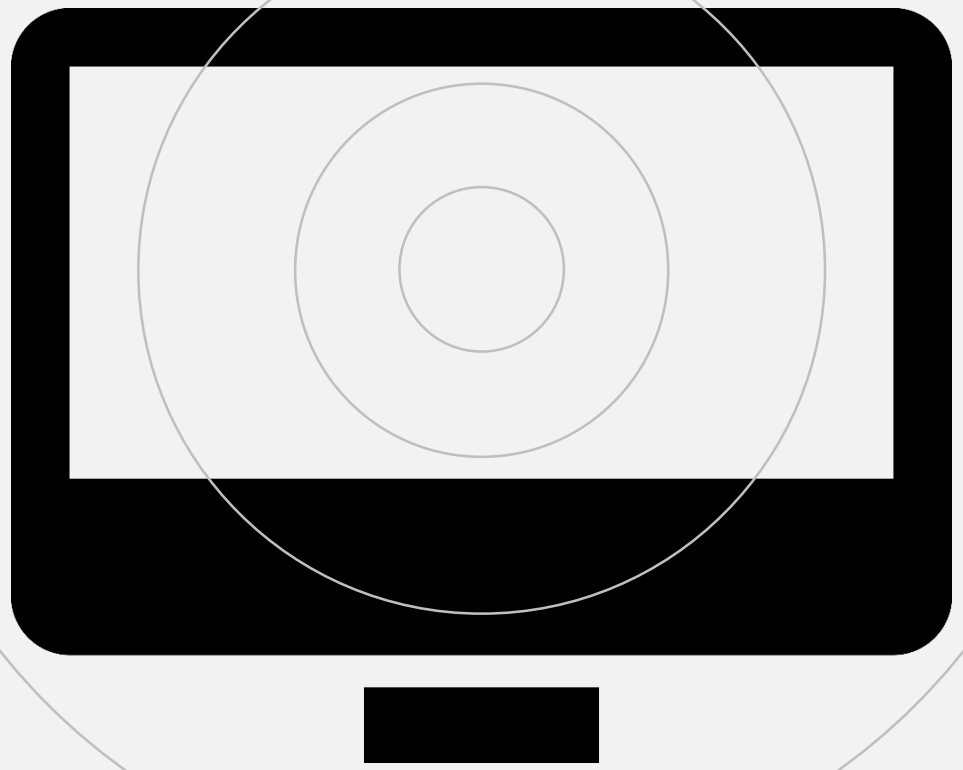
机器学习判断方向



如何直接通过无线监听得到其运动方向？

问题建模：分类问题

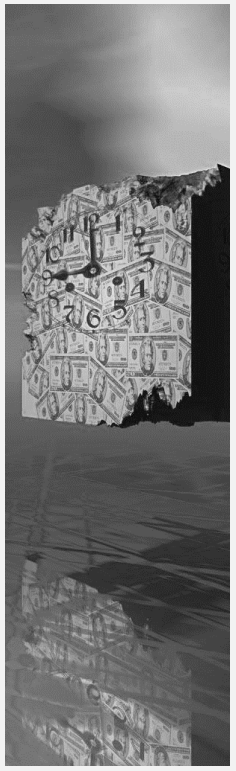
通过实时
监听通信
链路获取
数据特征



使用卷积
神经网络
判断上下
前后左右

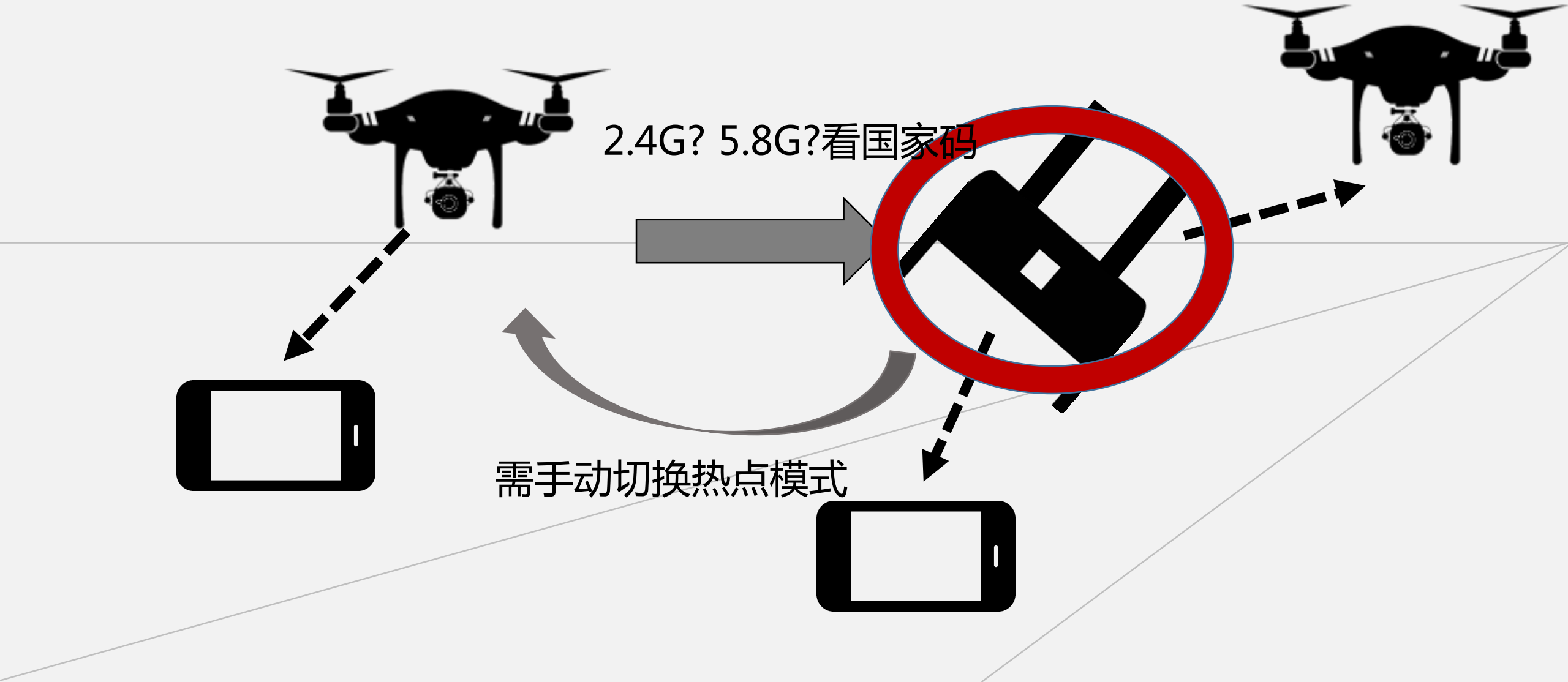
关键：提取怎样的特征？

DJI通信
链路分析

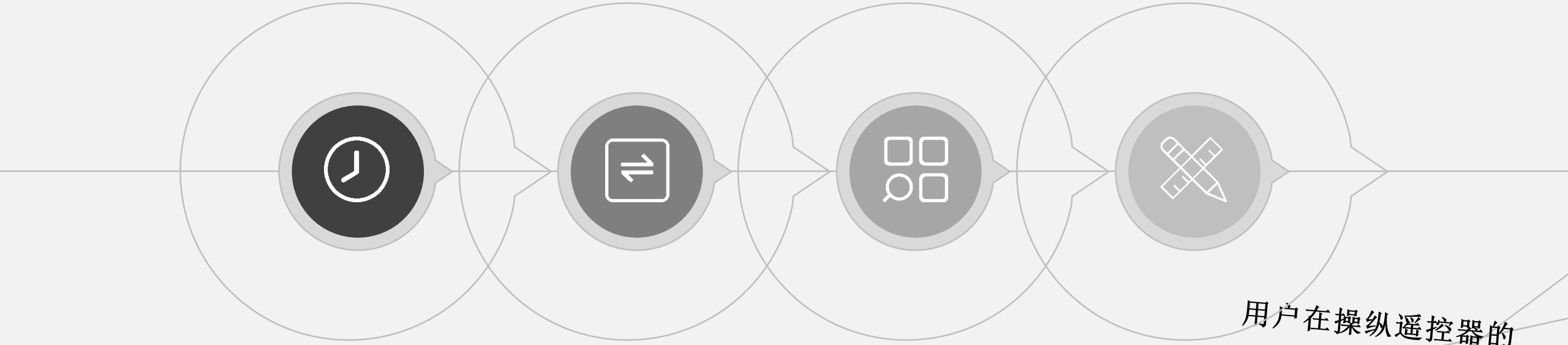


无人机运动
与信号特征
的关系

DJI Spark通信链路分析



DJI Spark通信链路分析



遥控器和无人机开机后，遥控器负责发送数据，无人机负责接收数据。它们通过共同的跳频序列的高速跳频来保持一个数据链路，链路故障有一定能力能迅速恢复。

无人机每**7ms**就会收到一次遥控器发出的**32**字节控制数据，控制数据只有一条命令一种格式，所有控制杆和开关的状态会一次性发送到无人机。无人机收到数据后会进行地址校验和**CRC**校验，确保数据是正确无误的。

用户在操纵遥控器的过程中，操控的行为和力度都会在**7ms**内通过那**32**字节控制数据反馈至无人机，接着由无人机的飞控程序来完成对应的飞行行为。

数据链路层协议：Enhanced ShockBurstTM

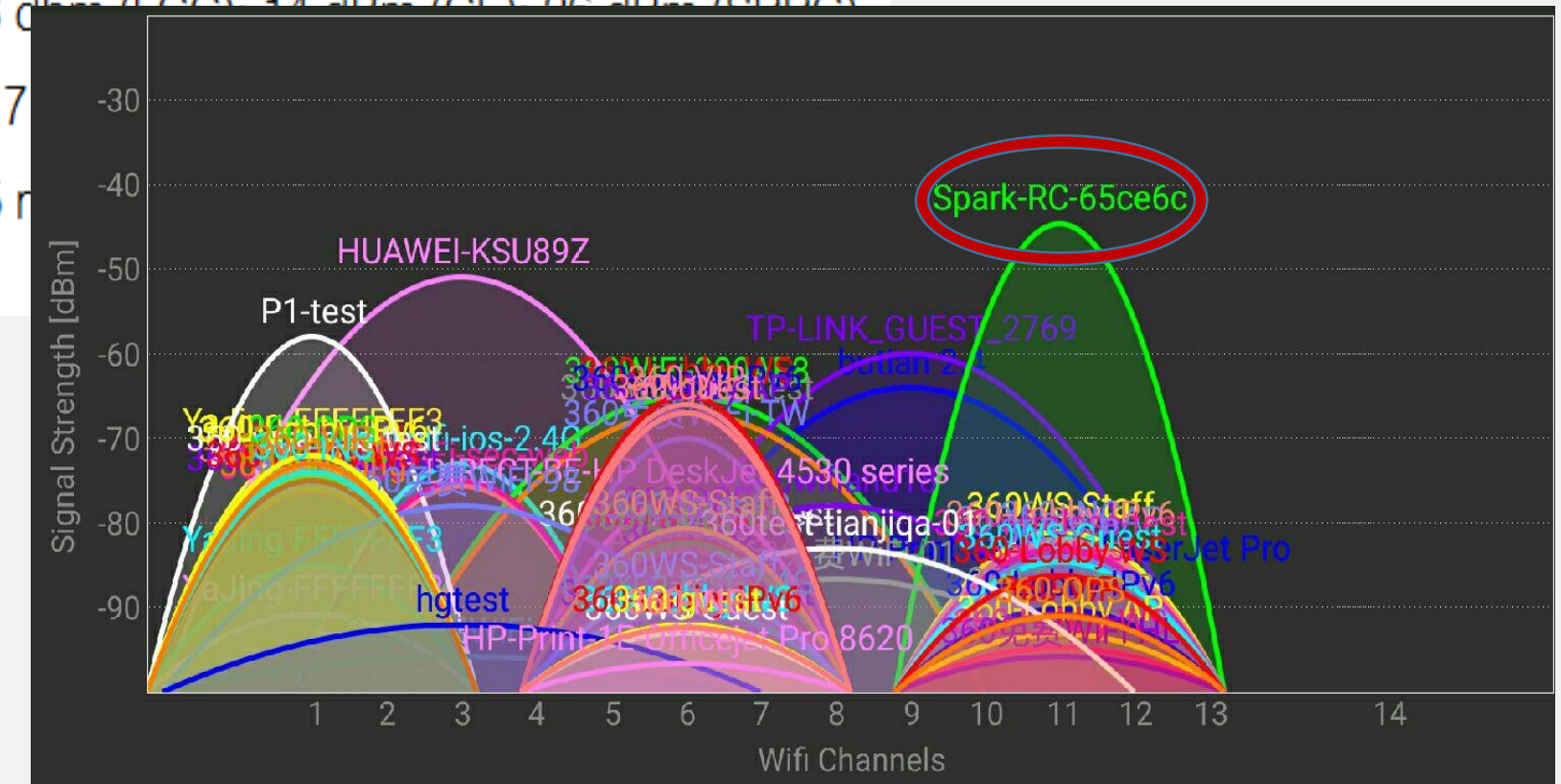
Preamble：自动生成，用于接收器同步数据流。01010101 或者10101010。
Address：接收器地址，程序控制。接收方通过检测该地址来解析数据。
PCF：包控制字段。6bit的payload长度，2bit的包标识，1bit的NO_ACK标识。
Payload：传输的用户数据。32bytes，占4/5.
CRC：自动计算。在接受方可屏蔽CRC校验过程。

本是可破解为二进制的，然而，大疆无人机在二月份将通信协议进行加密，采用WPA2进行加密WiFi，并采用防重放功能

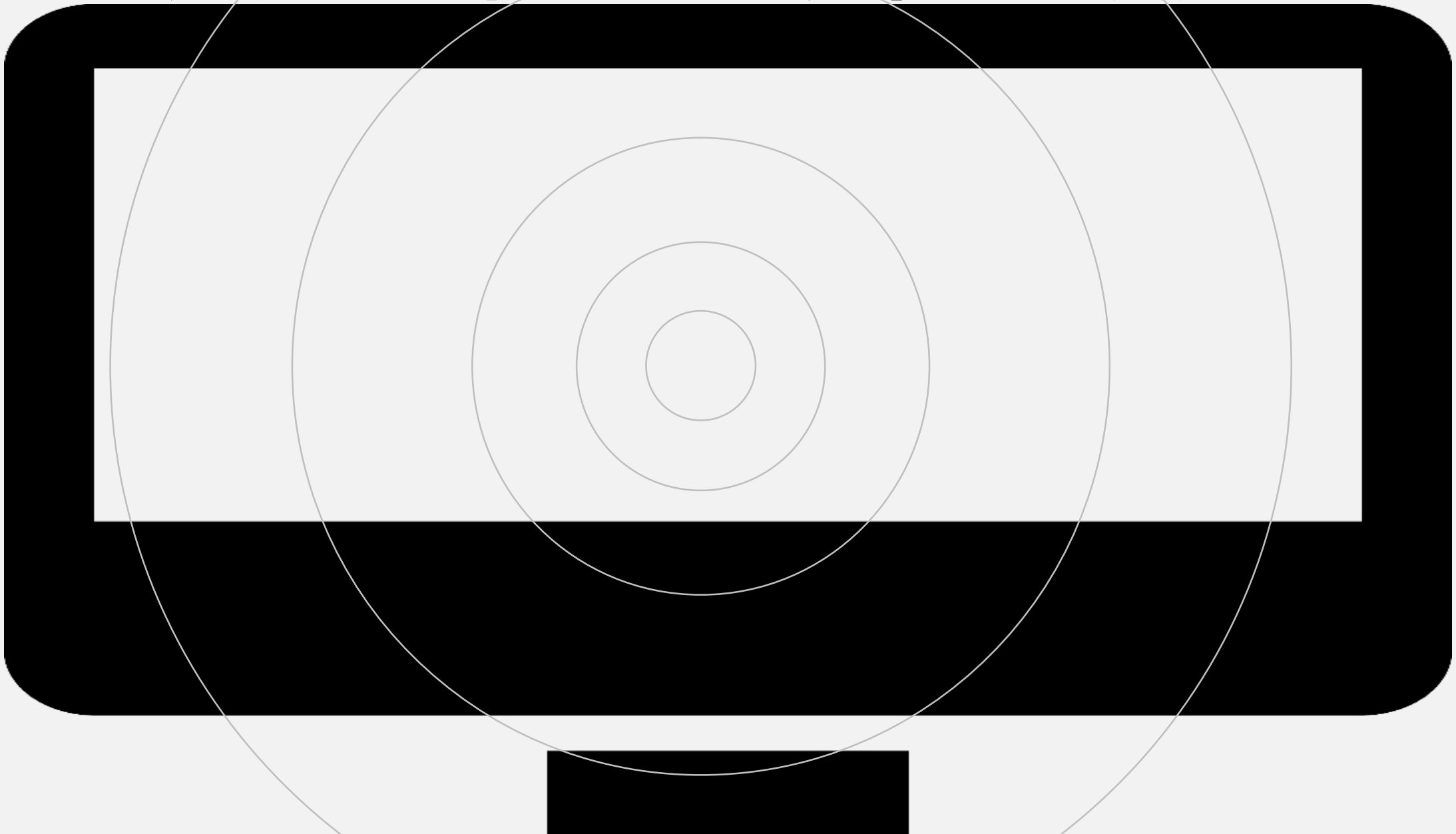
遥控器参数

工作频率	2.412-2.462 GHz； 5.745-5.825 GHz
信号有效距离 (无干扰、无遮挡)	2.4 GHz: 2000 m (FCC); 500 m (CE); 500 m(SRRC) 5.8 GHz: 2000 m (FCC); 300 m (CE); 1200 m (SRRC)
工作环境温度	0℃ 至 40℃
电 池	2970 mAh
发射功率 (平均 EIRP)	2.4 GHz: 26 dbm (FCC); 18 dBm (CE); 18 dBm (SRRC) 5.8 GHz: 28 d
工作电流 / 电压	950 mA @3.7
支持移动设备	厚度 6.5-8.5 r

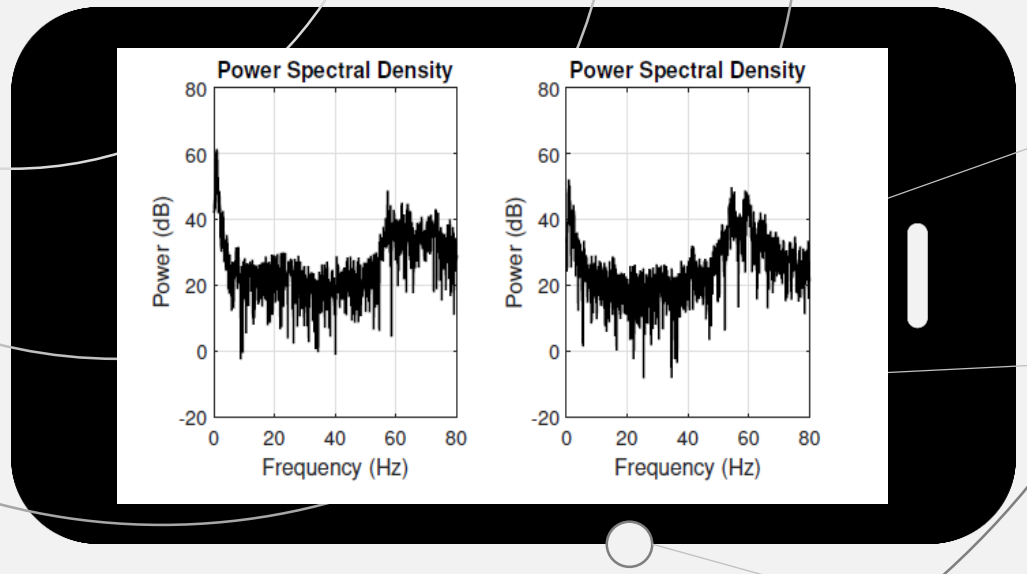
热点测量



发现：控制信号在功率上的反应



那么，Wi-Fi在信息层面值得监控吗？当然！



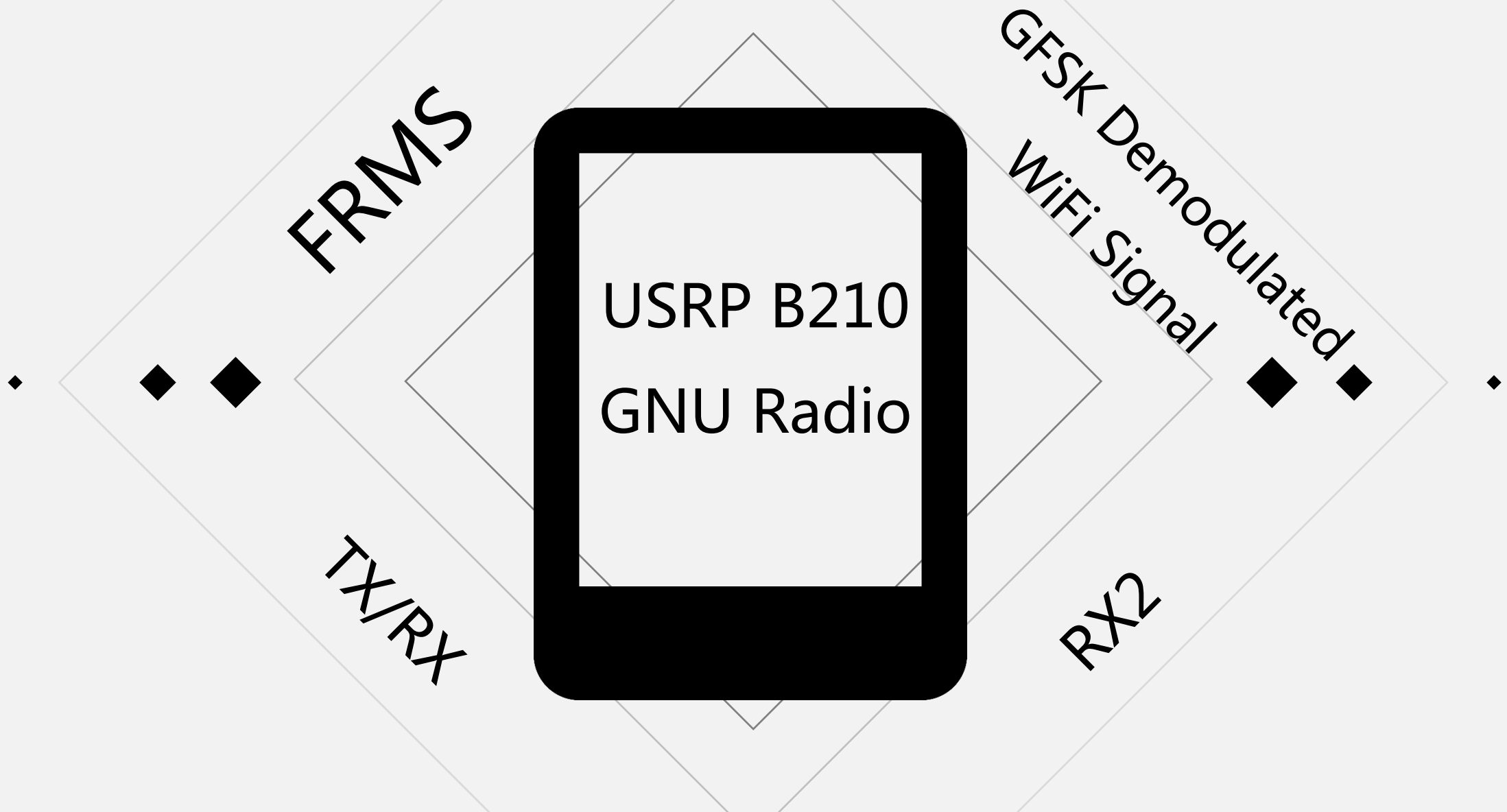
卷积神经网络能够深挖人所不能轻易发现的深层特征，从而绕过加密机制

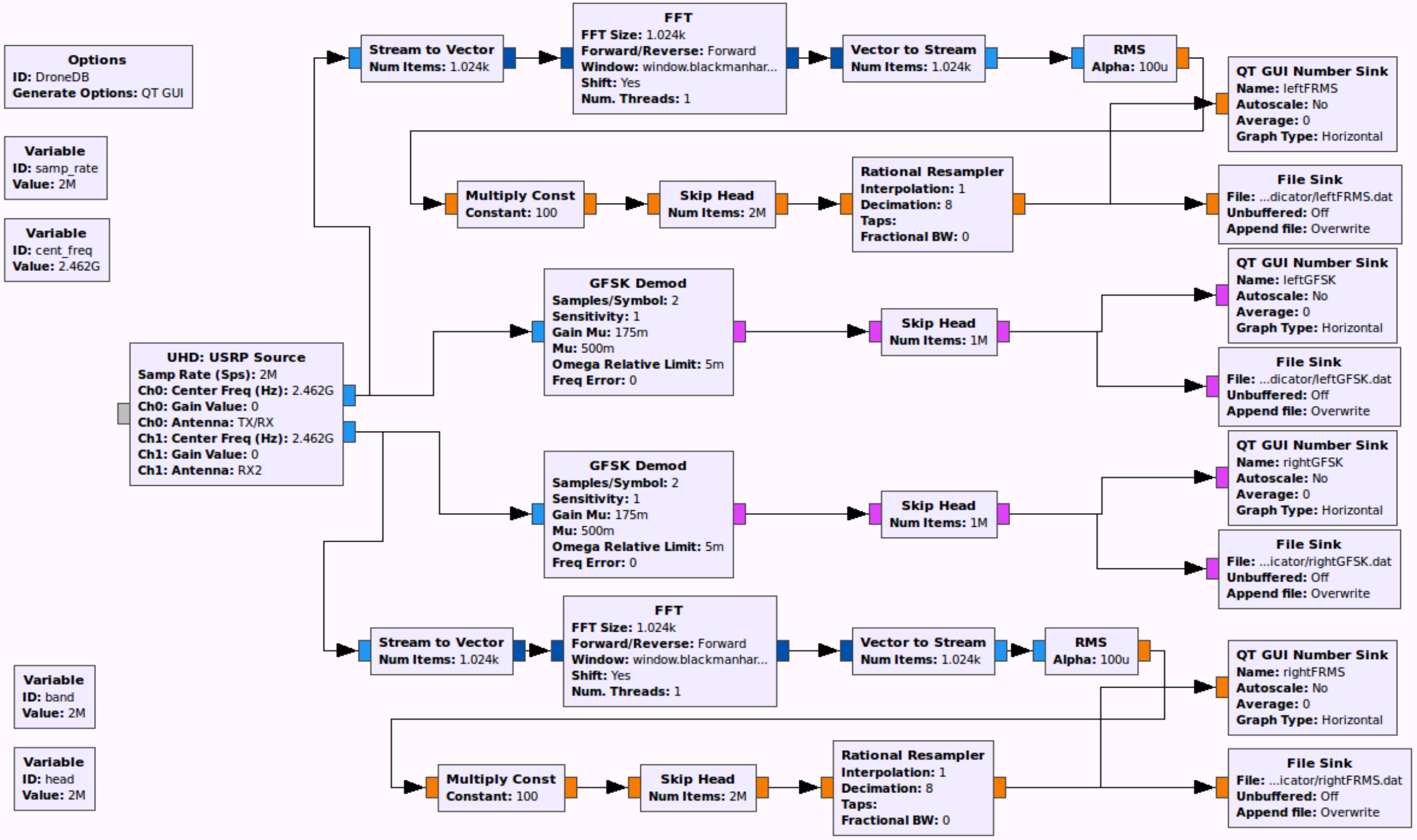
无人机的运动与RF频谱抖动大致相似*

GFSK解调后的码字拥有4/5的控制信号，即使加密，相同信息仍有相同哈希值

* MobiSys’17 Matthan: Drone Presence Detection by Identifying Physical Signatures in the Drone’s RF Communication

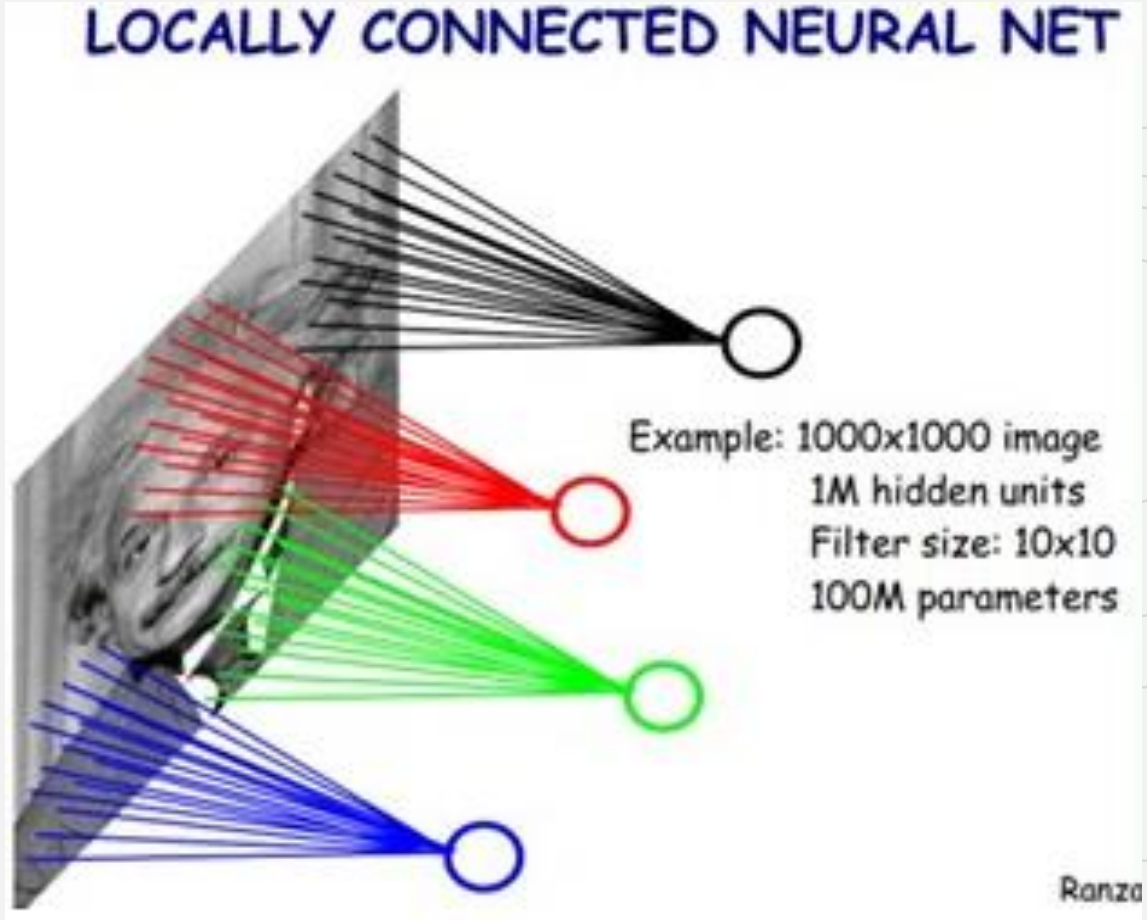
综上所述：选定的信号特征




Options
ID: DroneDB
Generate Options: QT GUI
Variable
ID: samp_rate
Value: 2M
Variable
ID: cent_freq
Value: 2.462G
Variable
ID: band
Value: 2M
Variable
ID: head
Value: 2M
UHD: USRP Source
Samp Rate (Sps): 2M
Ch0: Center Freq (Hz): 2.462G
Ch0: Gain Value: 0
Ch0: Antenna: TX/RX
Ch1: Center Freq (Hz): 2.462G
Ch1: Gain Value: 0
Ch1: Antenna: RX2
Stream to Vector
Num Items: 1.024k
FFT
FFT Size: 1.024k
Forward/Reverse: Forward
Window: window.blackmanhar...
Shift: Yes
Num. Threads: 1
Vector to Stream
Num Items: 1.024k
RMS
Alpha: 100u
QT GUI Number Sink
Name: leftFRMS
Autoscale: No
Average: 0
Graph Type: Horizontal
Multiply Const
Constant: 100
Skip Head
Num Items: 2M
Rational Resampler
Interpolation: 1
Decimation: 8
Taps:
Fractional BW: 0
File Sink
File: ...dicator/leftFRMS.dat
Unbuffered: Off
Append file: Overwrite
GFSK Demod
Samples/Symbol: 2
Sensitivity: 1
Gain Mu: 175m
Mu: 500m
Omega Relative Limit: 5m
Freq Error: 0
Skip Head
Num Items: 1M
QT GUI Number Sink
Name: leftGFSK
Autoscale: No
Average: 0
Graph Type: Horizontal
File Sink
File: ...dicator/leftGFSK.dat
Unbuffered: Off
Append file: Overwrite
GFSK Demod
Samples/Symbol: 2
Sensitivity: 1
Gain Mu: 175m
Mu: 500m
Omega Relative Limit: 5m
Freq Error: 0
Skip Head
Num Items: 1M
QT GUI Number Sink
Name: rightGFSK
Autoscale: No
Average: 0
Graph Type: Horizontal
File Sink
File: ...icator/rightGFSK.dat
Unbuffered: Off
Append file: Overwrite
Stream to Vector
Num Items: 1.024k
FFT
FFT Size: 1.024k
Forward/Reverse: Forward
Window: window.blackmanhar...
Shift: Yes
Num. Threads: 1
Vector to Stream
Num Items: 1.024k
RMS
Alpha: 100u
QT GUI Number Sink
Name: rightFRMS
Autoscale: No
Average: 0
Graph Type: Horizontal
Multiply Const
Constant: 100
Skip Head
Num Items: 2M
Rational Resampler
Interpolation: 1
Decimation: 8
Taps:
Fractional BW: 0
File Sink
File: ...icator/rightFRMS.dat
Unbuffered: Off
Append file: Overwrite

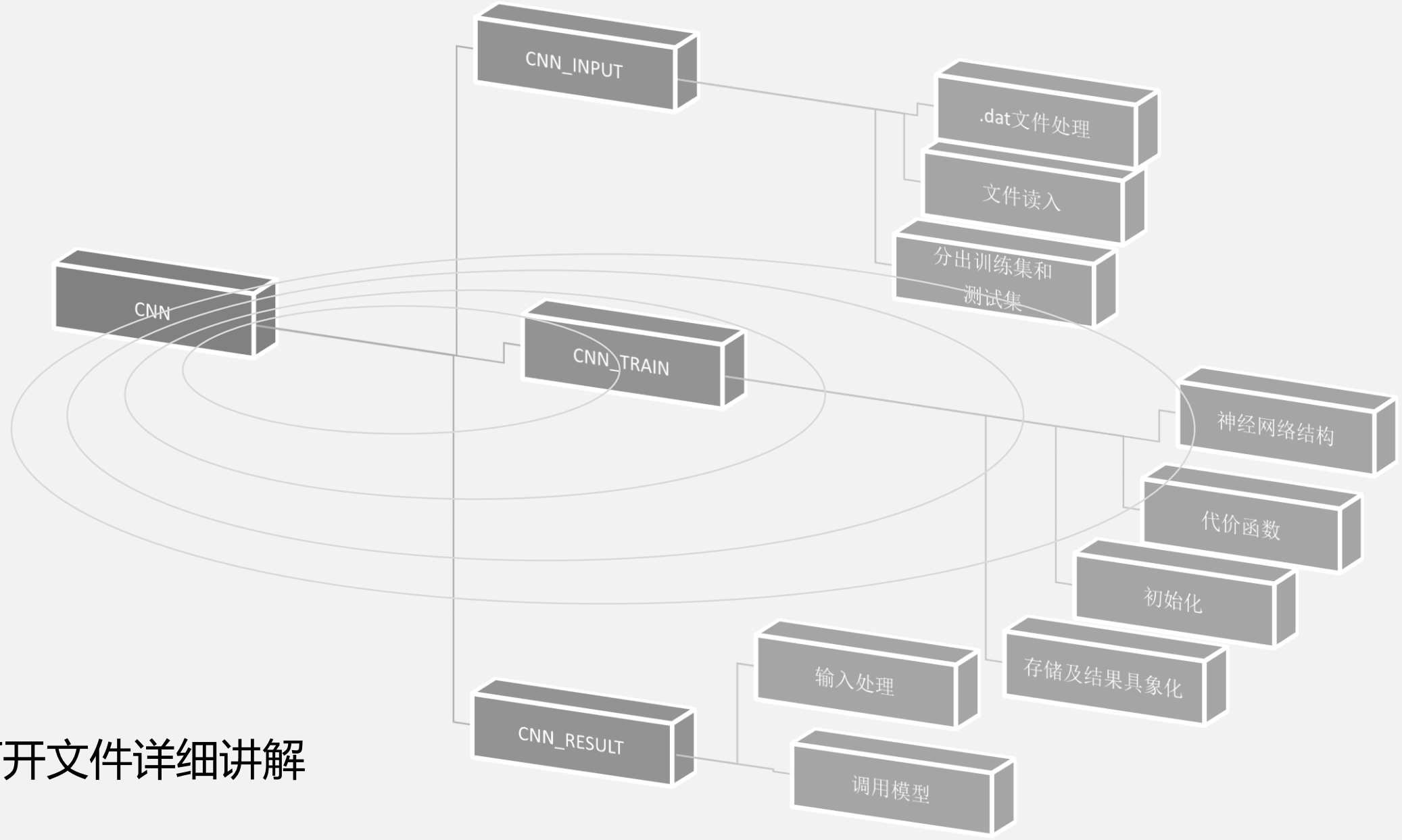
雷达

卷积神经网络介绍



- 基本处理单位为图
- 通过扫描挖掘特征
- 效果超好的黑箱

代码结构介绍



打开文件详细讲解

雷达

卷积神经网络结构

不断调整模型

- 3个卷积层
- 3个池化层
- 1个全连接层

有坑勿踩

.dat文件读入

十进制还是二进制？

Byte格式与Complex格式的区别？

过拟合问题

Dropout函数？

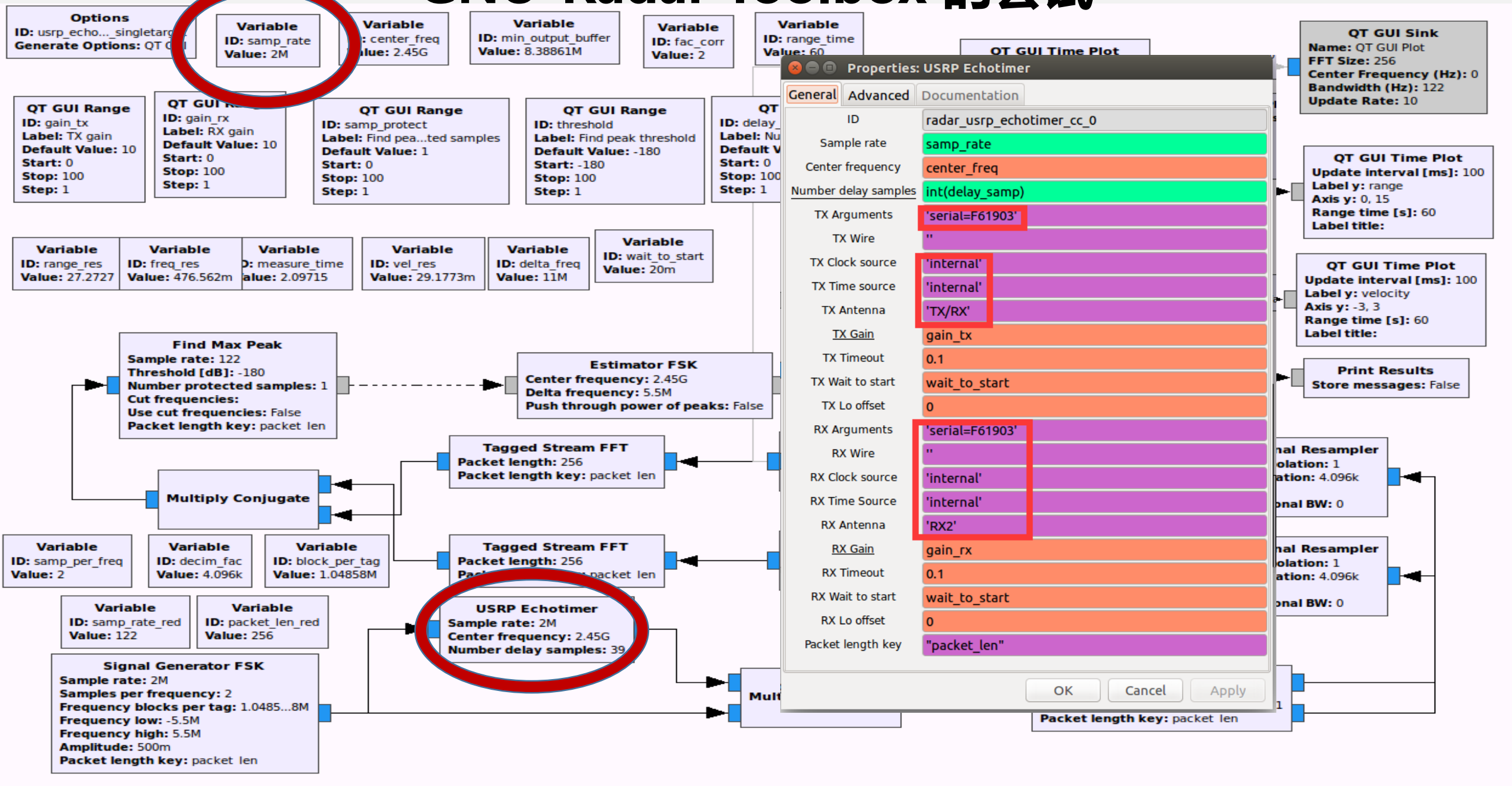
数据越纯净越好？

Local Optimal问题

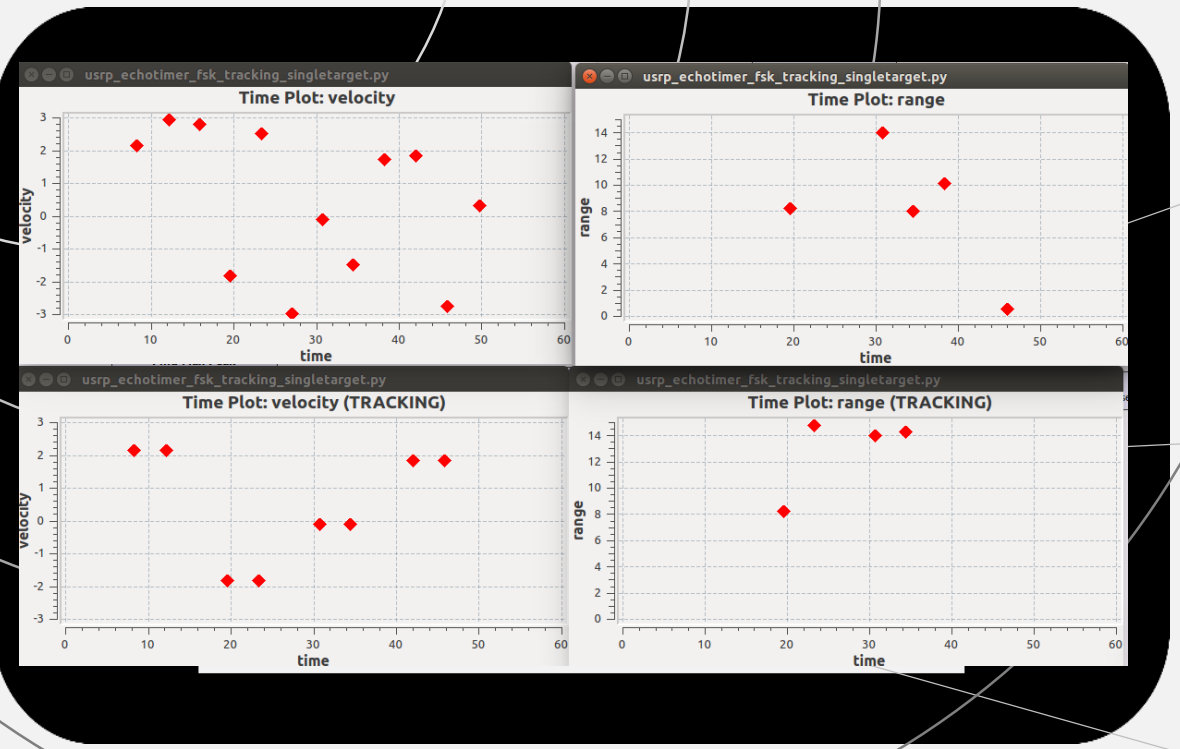
怎样的Learning Rate比较合适？

如何应对随机的初值？

GNU-Radar Toolbox 的尝试



效果不尽如人意，原因是？



小目标受地物杂波的影响，探测难度非常大

运动的小目标需要云台快速配合定向天线，具有较高精度要求

大疆精灵系列无人机的RCS(散射截面积)是0.01

PART 03

数据分析及解读

实验设定：数据接收 Experimental Setups：Data Receiving

1. 硬件

- HP ProBook (Intel i5-6200U CPU@2.30GHz 2GB RAM)
- USRP B210 (2x2 MIMO 70MHz-6GHz)
- DJI Spark + Remote Controller C2
- 雷达型定向天线 *2（10dB）

2. 软件

- Ubuntu 16.04
- GNU Radio Companion 3.7.10
- Python 2.7.11

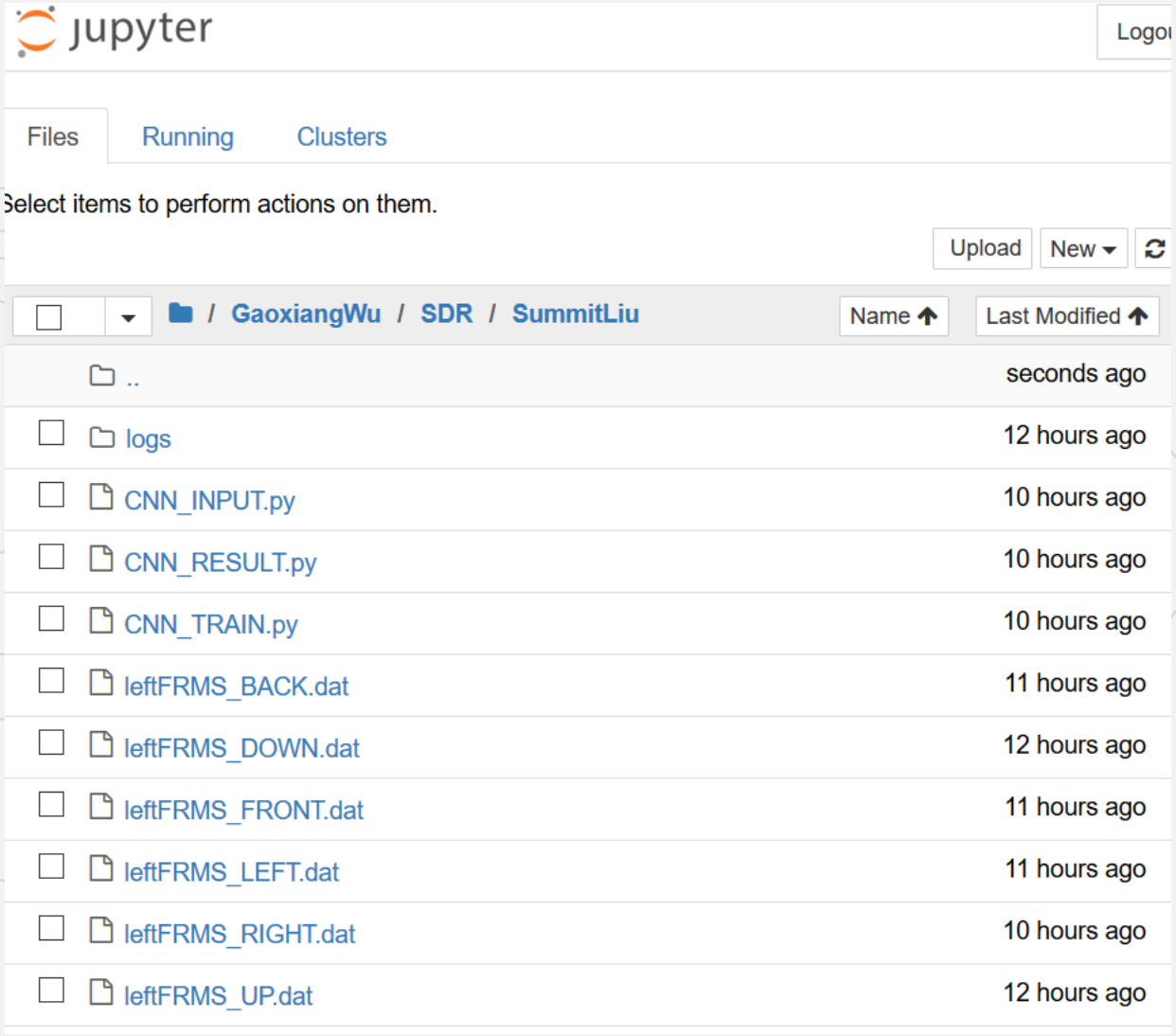
实验设定：数据处理 Experimental Setups：Data Processing

1. 硬件

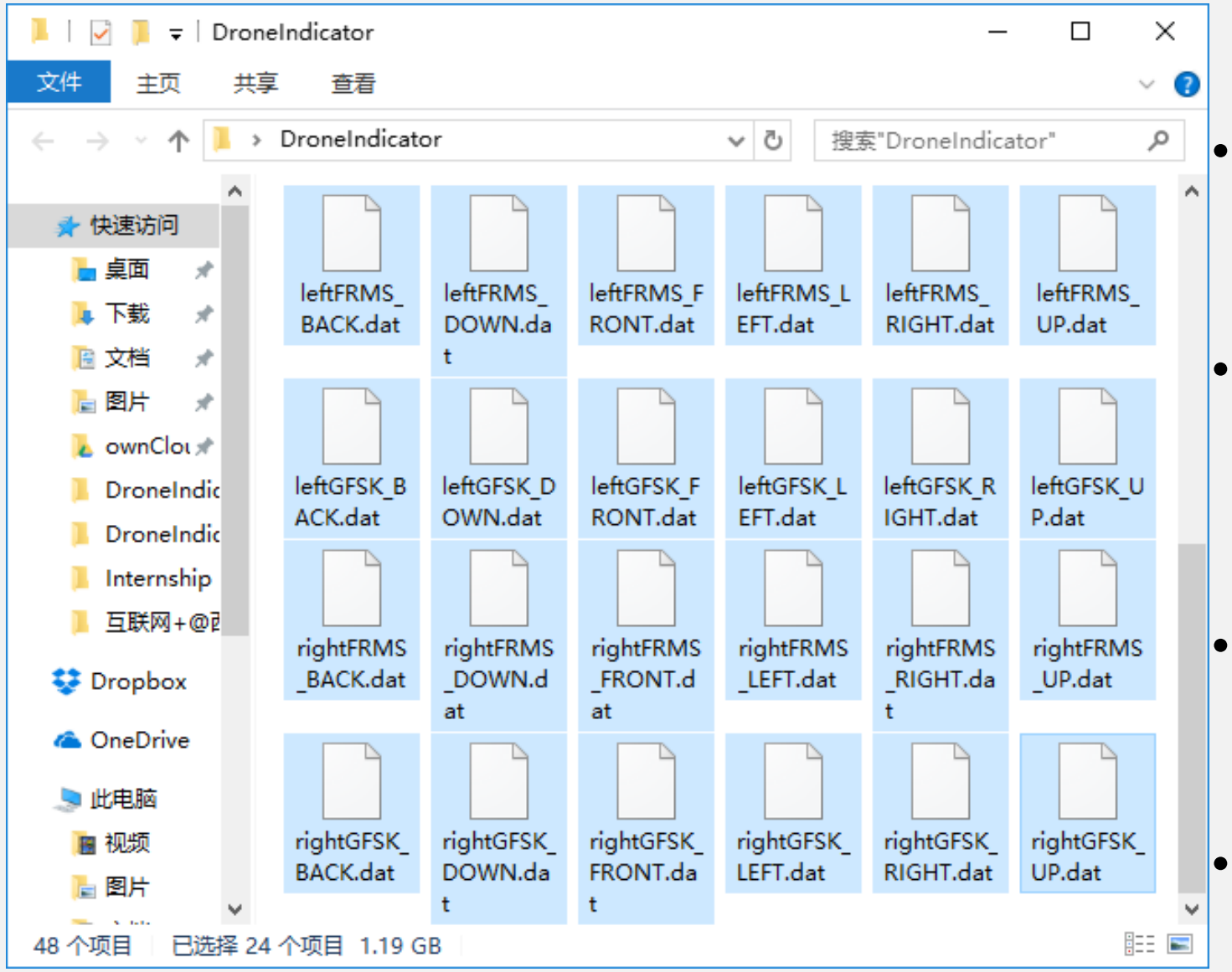
- **Inspur server (24 Cores Intel Xeon CPU E5-24200 @ 1.90GHz, 64GB RAM)**

2. 软件

- **Red Hat 4.4.7-11**
- **Jupyter 6.0**
- **TensorFlow 1.1.0**
- **Python 3.6.1**

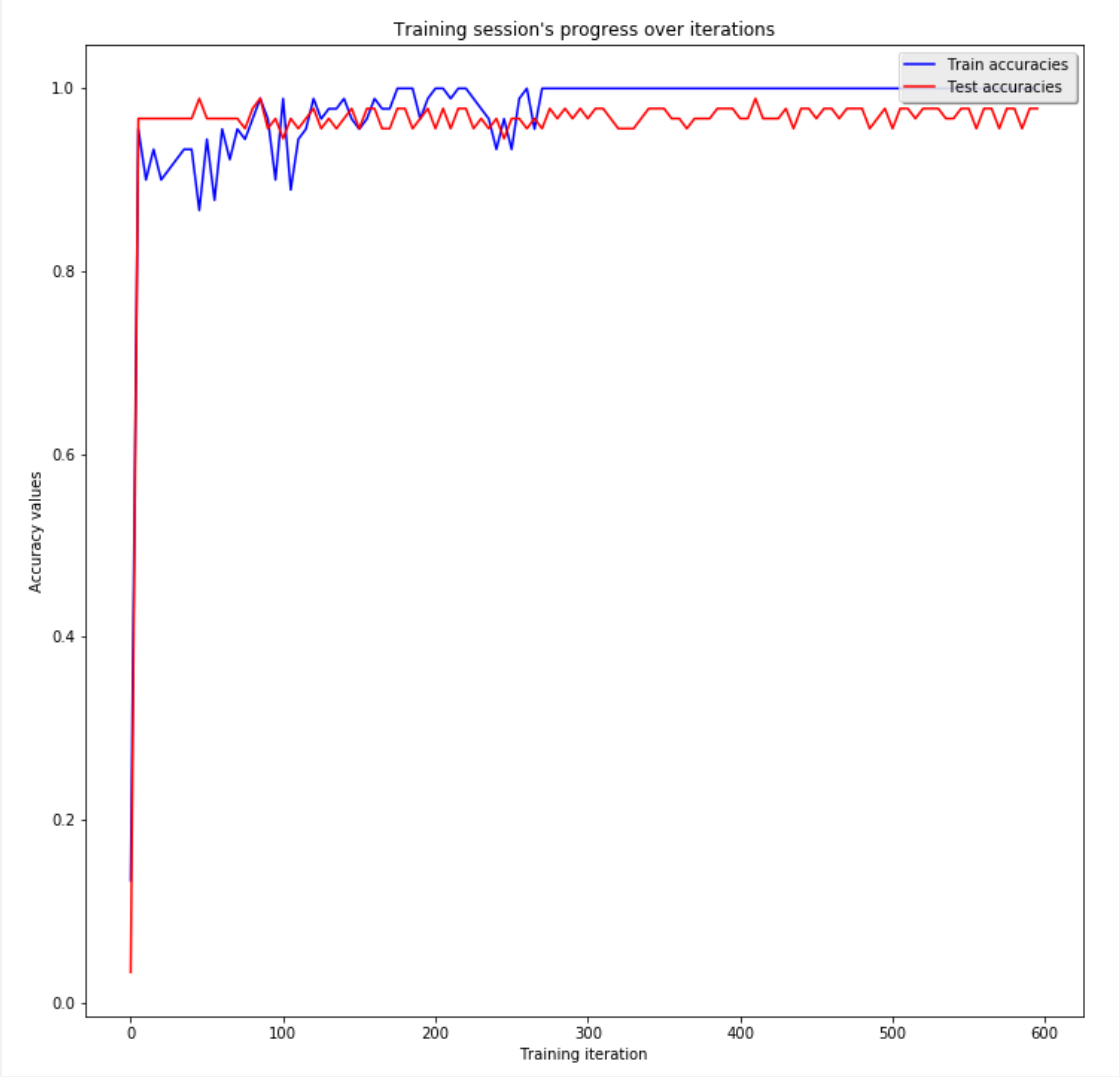


数据量 Data Amount



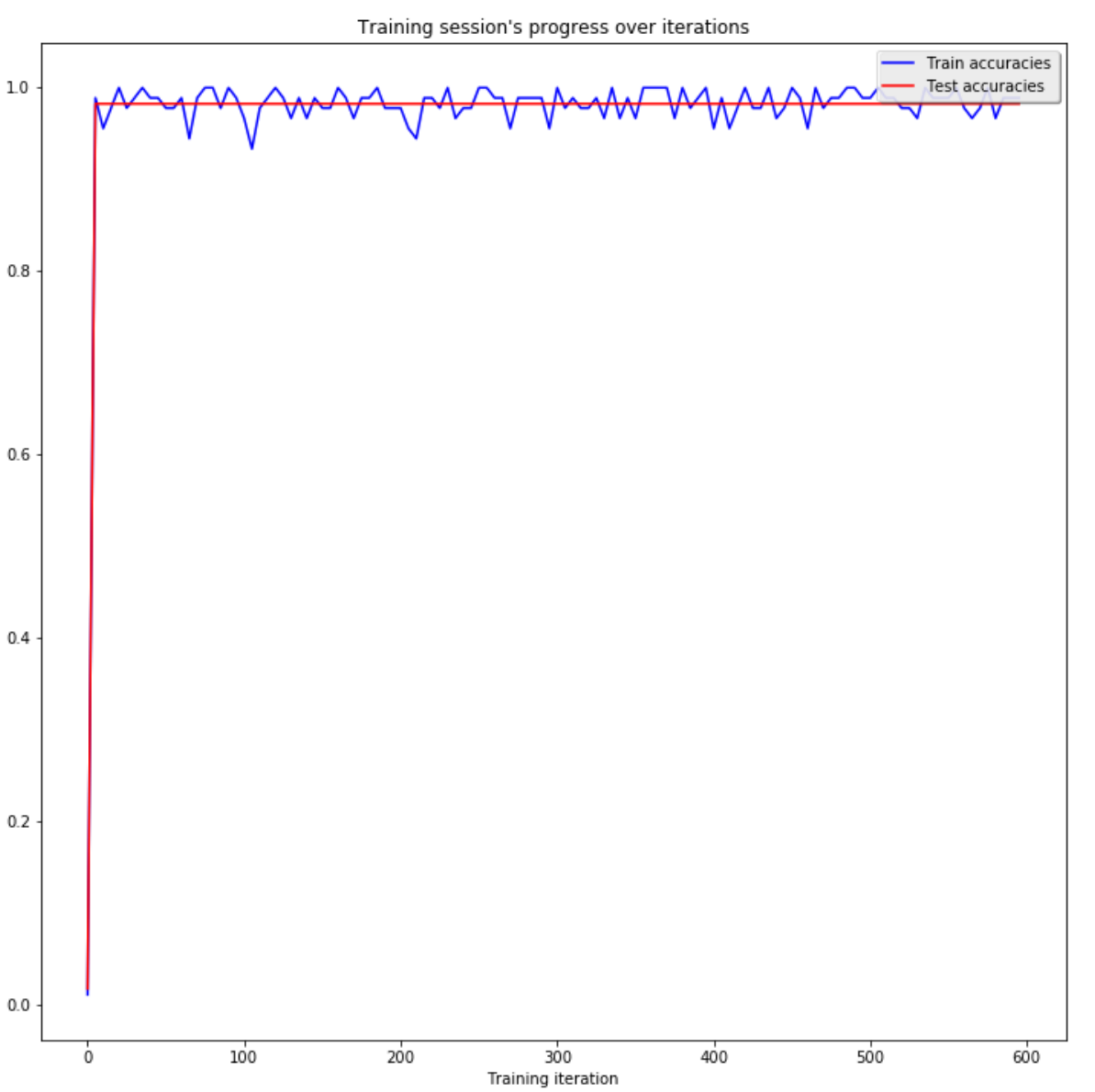
- 分类：UP、DOWN、FRONT、BACK、LEFT、RIGHT 6个类别
- 每个类别包含leftFRMS、leftGFSK（TX/RX），rightFRMS，rightGFSK（RX2）四种信号特征
- 每类别每种信号特征各50MB，共1.2GB
- 其中120MB为测试集，余者皆训练集

单一特征（leftFRMS）二分（UP & DOWN）结果



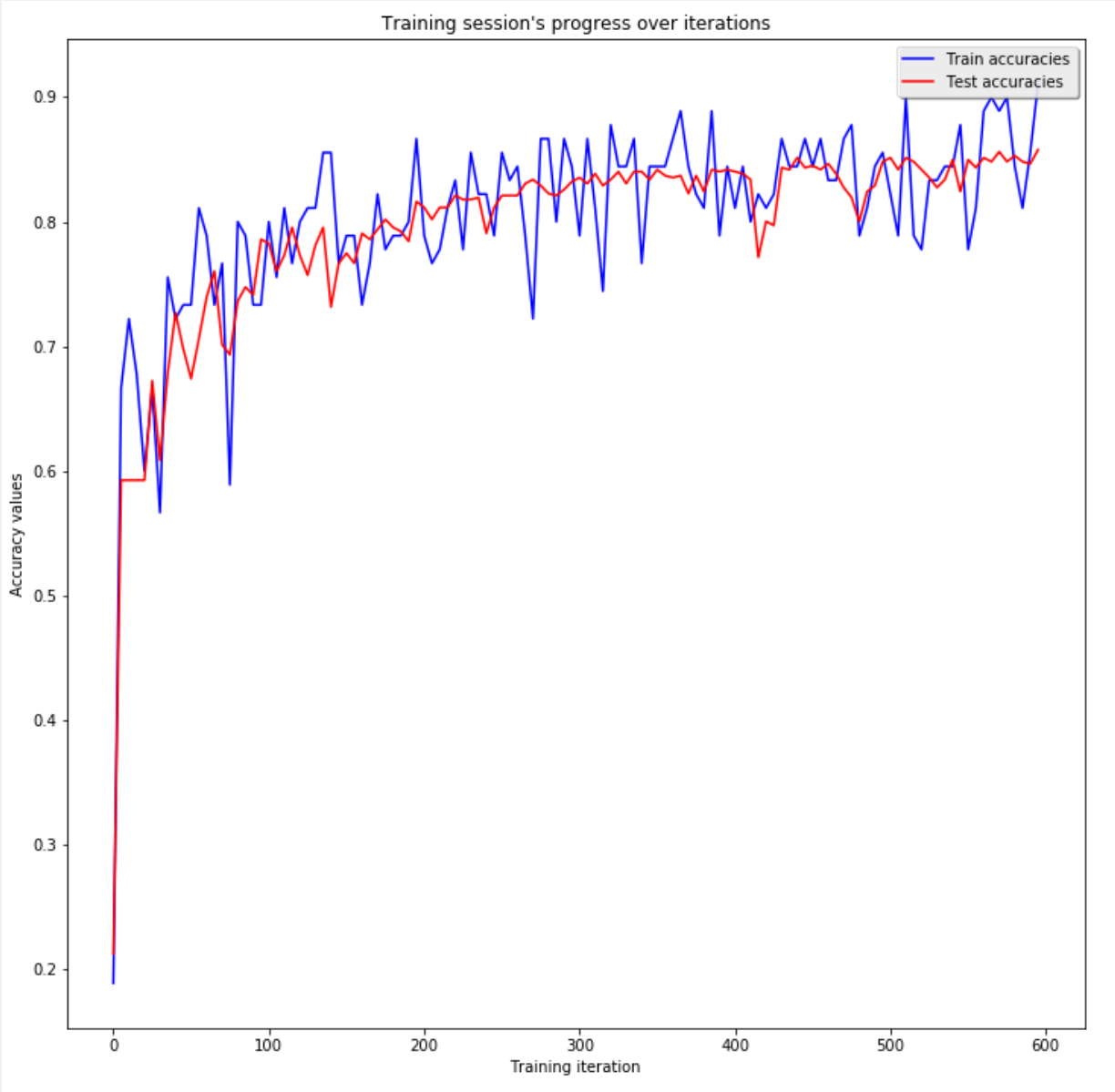
- 训练过程耗时**327.3s**
- 模型单独进行一次判断平均耗时**3064ms**
- 训练集约**300**次重复后正确率稳定在**100%**
- 测试集正确率基本稳定在**95.3%**至**97.8%**之间

单一特征（leftGFSK）二分（UP & DOWN）结果



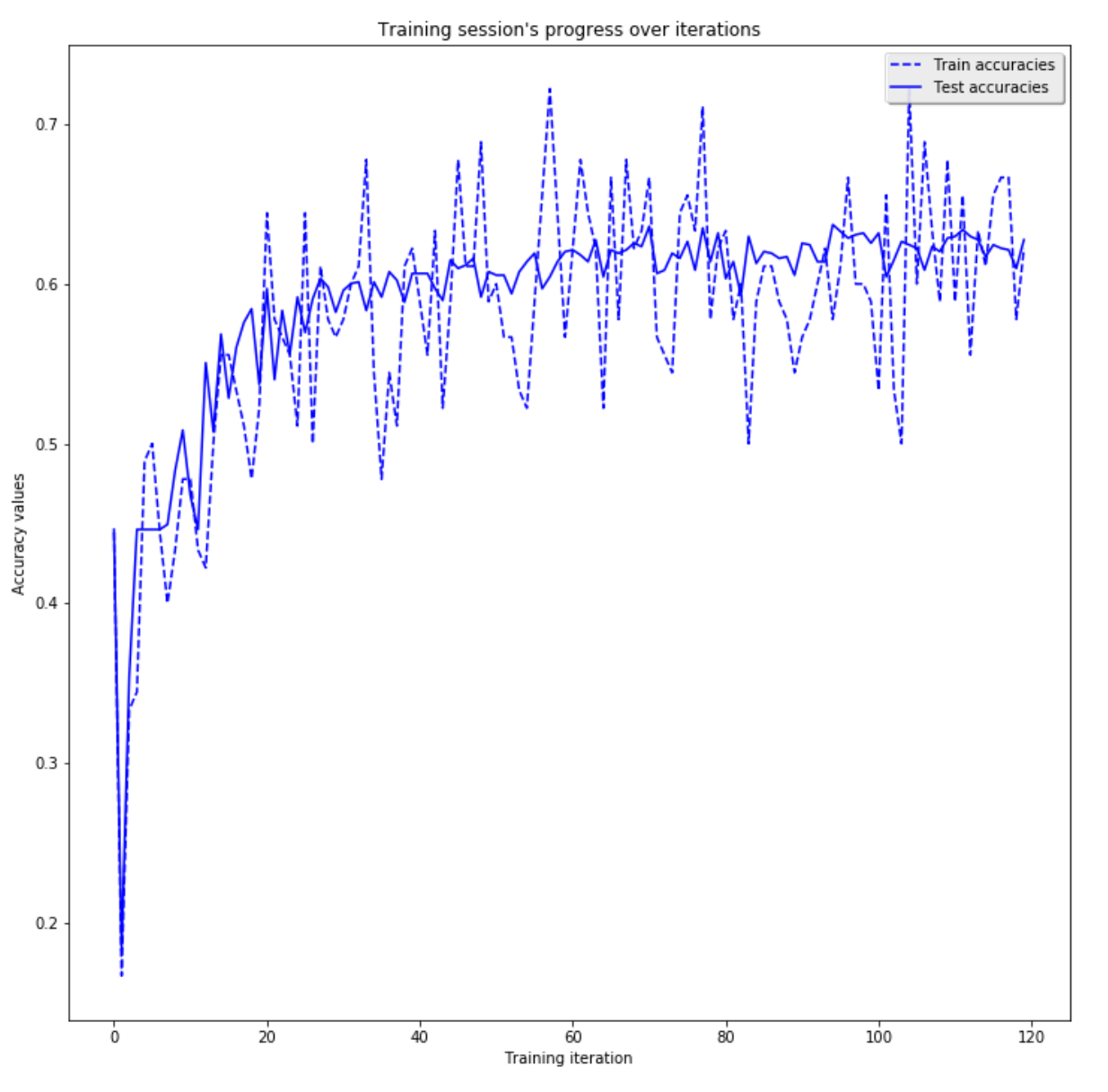
- 训练过程耗时**329.9s**
- 模型单独进行一次判断平均耗时**3173ms**
- 测试集正确率稳定在**98.2%**
- **GFSK**包含的判断信息比功率更多

单一特征（rightFRMS）四分（FRONT & BACK & UP & DOWN）结果



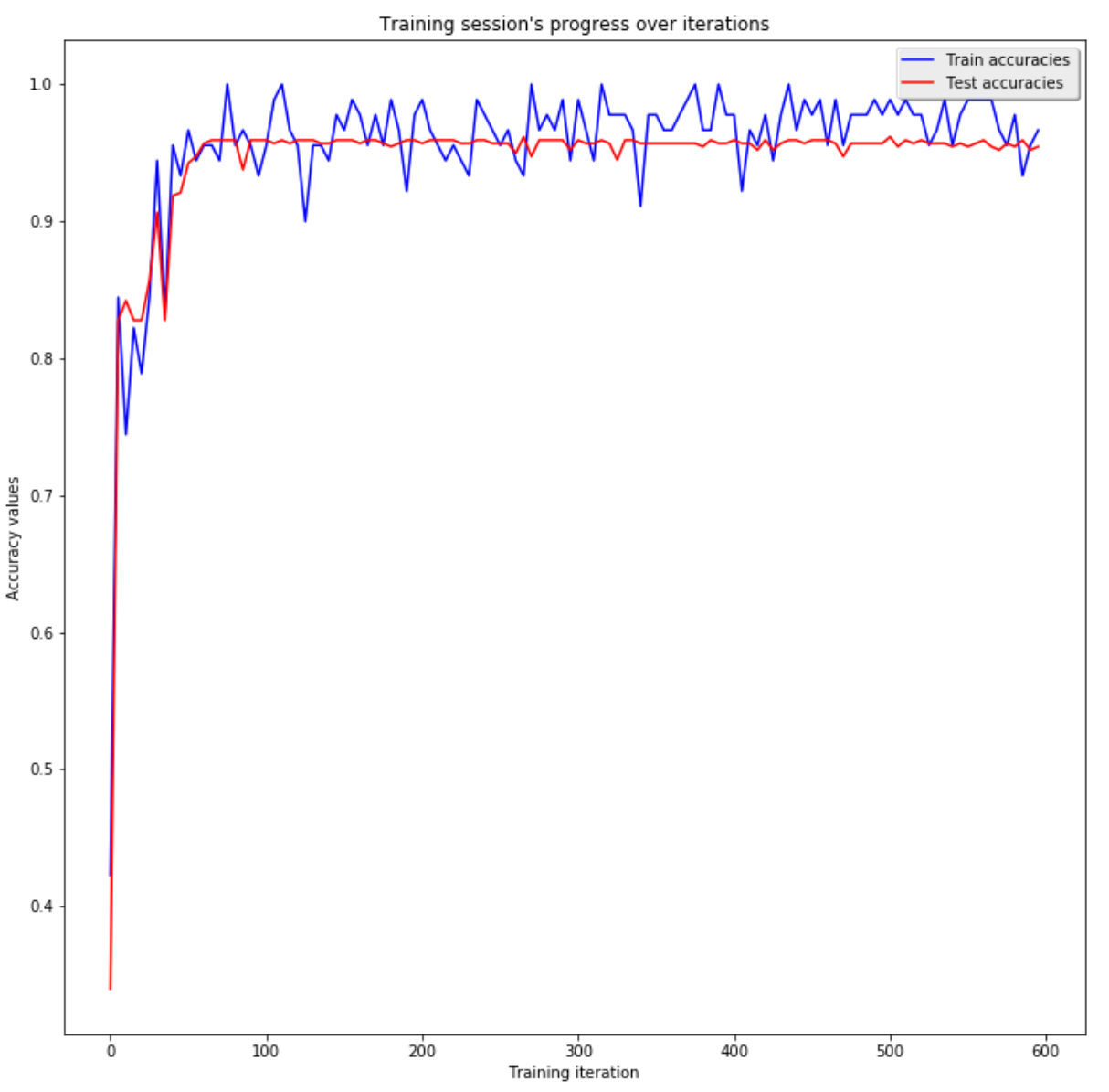
- 训练过程耗时612.5s
- 模型单独进行一次判断平均耗时4256ms
- 训练集正确率在90%上下波动
- 测试集正确率基本稳定在85.2%

单一特征（rightFRMS）六分结果



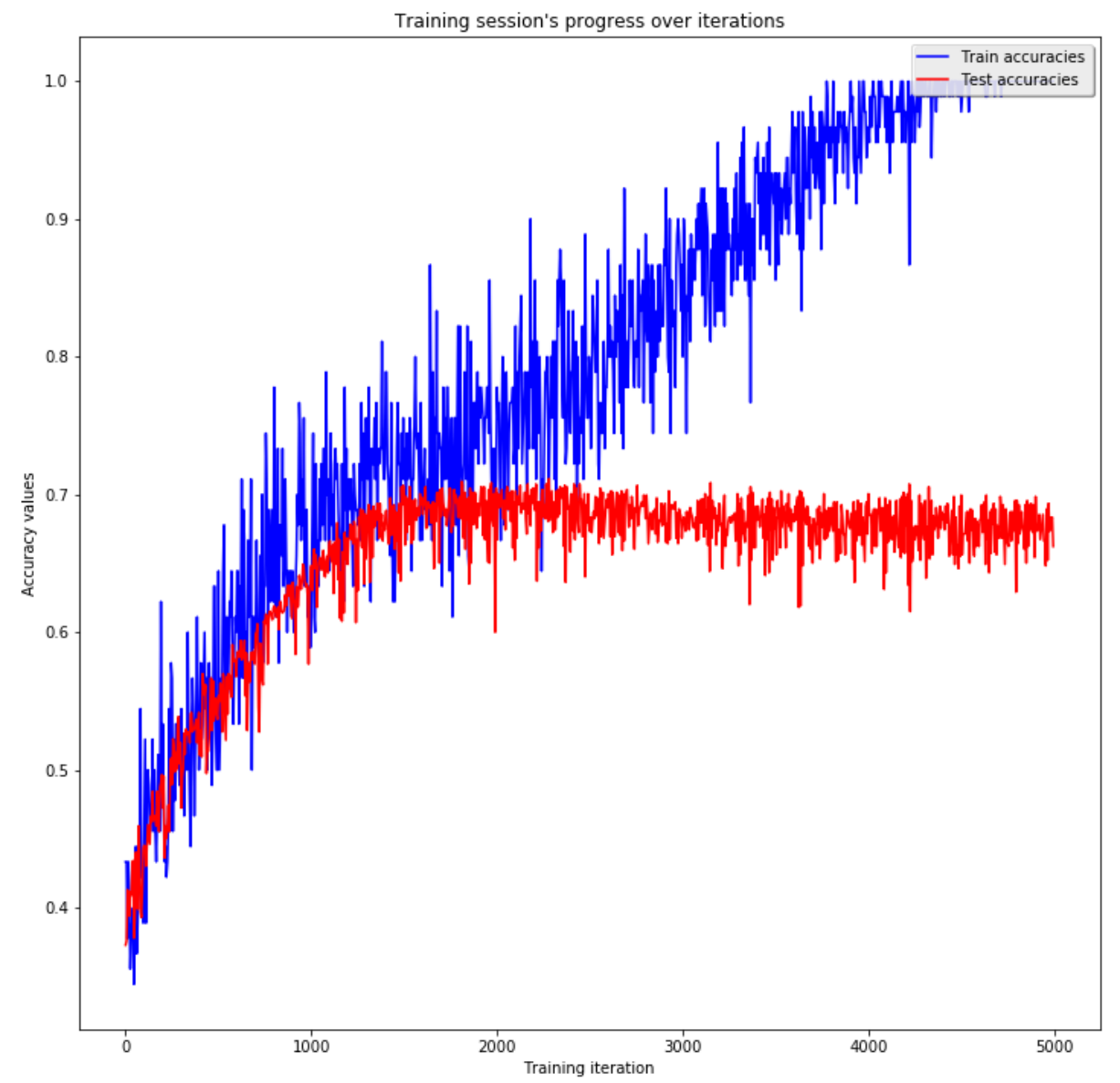
- 训练过程耗时**874.7s**
- 模型单独进行一次判断平均耗时**4827ms**
- 训练集正确率在**65%**上下波动
- 测试集正确率基本稳定在**62.3%**

双特征（leftFRMS & rightFRMS）对比说明



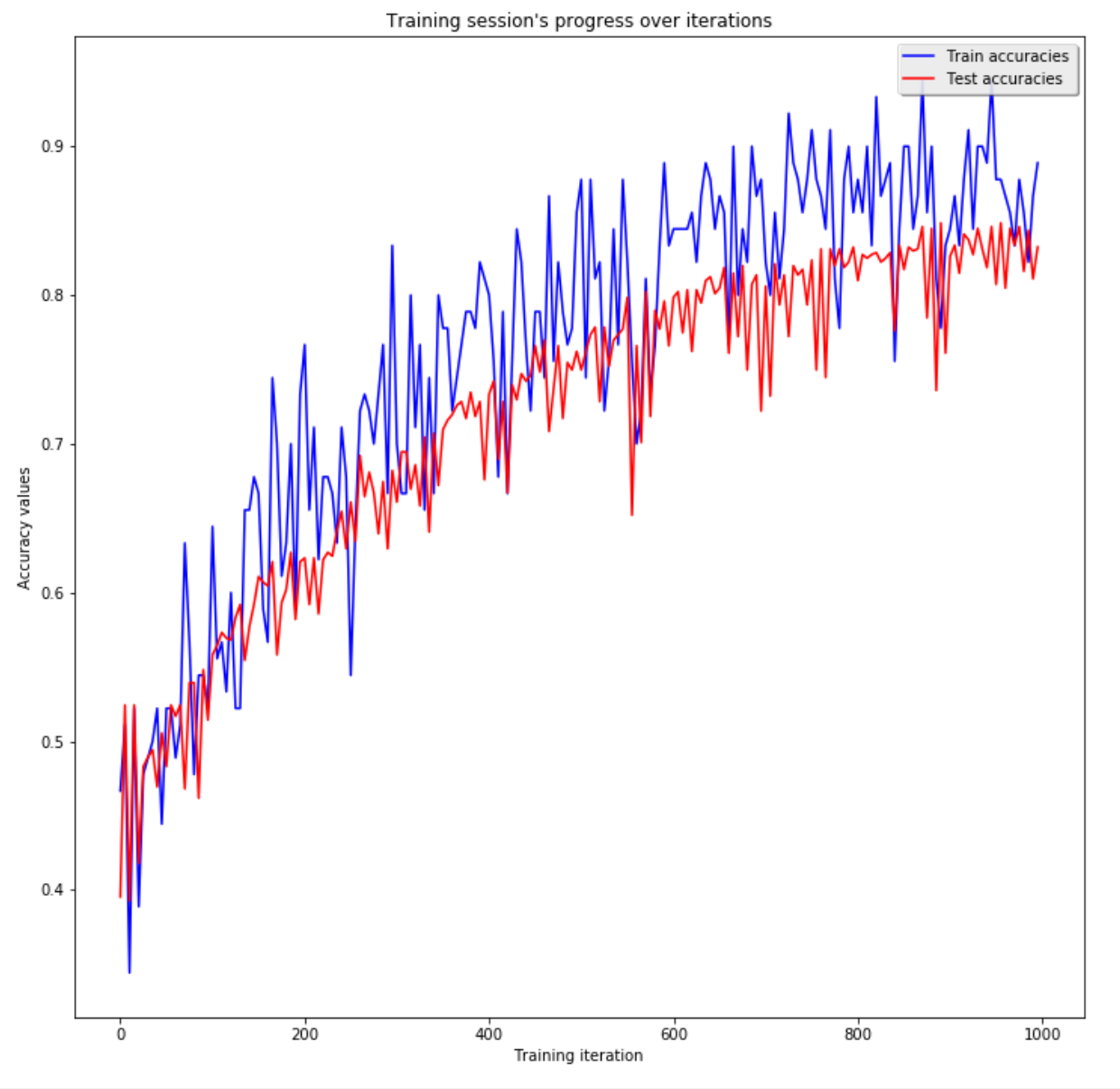
- 训练集正确率在**97%**上下波动
- 测试集正确率基本稳定在**95.7%**
- 说明两根天线接收到的**FRMS**大致相同又因为距离和摆放原因有少许不同
- 可以利用这种不同辅助判断

双特征（leftFRMS & rightFRMS）六分结果



- 训练集正确率持续走高
- 测试集正确率基本稳定在**68.9%**左右
- 说明测试集与训练集在划分时存在部分偏差，与选取特征同样有关
- 存在部分过拟合现象

四特征六分结果



- 训练集正确率在86%上下波动
- 测试集正确率基本稳定在83%
- 基本满足日常需求
- 左移右移较难判断，污染了数据库

意义：Inference Attack On Wireless Channels

防御手段？

1 射频收发两端加入噪声添加与去除防止学习

2 使通信协议的传输过程能按照随机生成的方法进行变动

3 静默飞行，采取非无线的通信方式（光桥等）

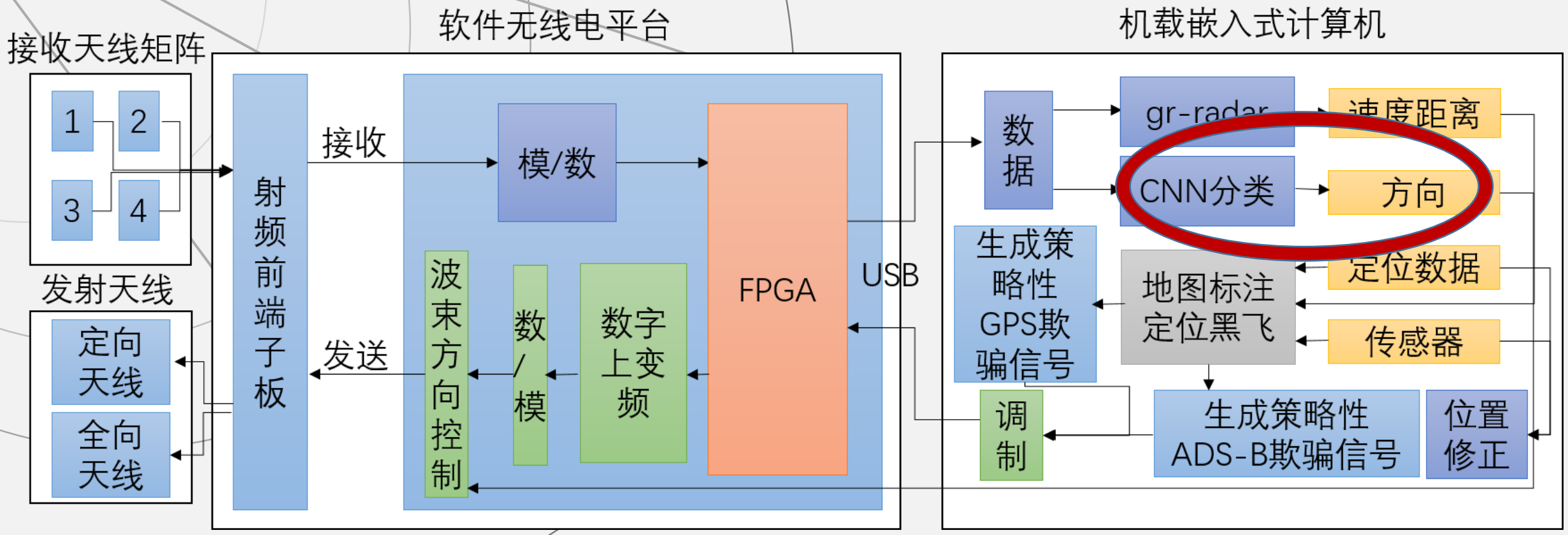
4 你认为呢？

PART 04

未来展望及预期

未来的工作

刑天：基于无人机的无线电反无人机系统



THANKS

DDI : Deep Learning in Drone Direction Indication

汇报：刘诗楠

时间：2017年8月25日